AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) Mobile telephone handset ~~(1)~~, ~~characterised in that it~~ comprises:

- a storage support ~~(2)~~ which is secured against fraudulent access, which stores the IMEI ~~(21)~~ of the handset;

- a connector ~~(3)~~ for a secure electronic module ~~(31)~~, which is associated with an operator;

- a handset ~~(1)~~ operating system ~~(4)~~, which controls authentication of the IMEI storage support ~~(2)~~ by a secure electronic module which is connected to the aforementioned connector in order to establish a secure communication channel ~~(6)~~ between the storage support and the module and transmission of the IMEI over the secure channel to the secure electronic module.

2. (Currently Amended) Mobile telephone handset ~~(1)~~ according to claim 1, ~~characterised in that~~ wherein the operating system ~~(4)~~ controls the transmission of the IMEI to a mobile telephone operator ~~(5)~~ by means of a secure OTA channel.

3. (Currently Amended) Handset according to ~~any one of the preceding claims, characterised in that~~ claim 1, wherein it comprises a secure electronic module ~~(31)~~ associated with the operator connected to the connector.

4. (Currently Amended) Handset according to claim 3, ~~characterised in that~~ wherein the secure electronic module is a UICC.

5. (Currently Amended) Handset according to claim 3 ~~or 4, characterised in that~~ , wherein the operating system controls the authentication of the secure module by the storage support.

6. (Currently Amended) Handset according to claim 5, ~~characterised in that~~ wherein the secure electronic module and the storage support store encryption keys ~~(22)~~ that are adapted to securing the secure communication channel ~~(6)~~.

7. (Currently Amended) Handset according to ~~any one of the claims from 3 to 6, characterised in that~~ claim 3, wherein the secure module ~~(31)~~ blocks the use of the handset when a false IMEI is detected.

8. (Currently Amended) Method of securing the IMEI of a mobile telephone handset ~~(1)~~ comprising the following steps:

- authenticating a secure storage support by memorising its IMEI ~~(21)~~, by a secure electronic module ~~(31)~~ associated with the operator and inserted in a connector ~~(3)~~ of the handset, in order to establish a secure channel between the storage support and the secure module;
- transmitting the IMEI ~~(21)~~ from the storage support to the secure module over the secure channel.

9. (Currently Amended) Method according to claim 8, ~~characterised in that~~ wherein the secure module ~~(31)~~ also transmits the IMEI to a mobile telephone operator over a secure OTA channel.

10. (Currently Amended) Method according to claim 9, ~~characterised in that~~ wherein the operator compares the IMEI with a black list ~~(7)~~ of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.

11. (Currently Amended) Method according to ~~any one of the claims from 8 to 10, characterised in that~~ claim 8, wherein the secure module blocks the use of the handset when a false IMEI is detected.

12. (New) Handset according to claim 4, wherein the operating system controls the authentication of the secure module by the storage support.

13. (New) Handset according to claim 4, wherein the secure module blocks the use of the handset when a false IMEI is detected.

14. (New) Handset according to claim 5, wherein the secure module blocks the use of the handset when a false IMEI is detected.

15. (New) Handset according to claim 6, wherein the secure module blocks the use of the handset when a false IMEI is detected.

16. (New) Method according to claim 9, wherein the secure module blocks the use of the handset when a false IMEI is detected.

17. (New) Method according to claim 10, wherein the secure module blocks the use of the handset when a false IMEI is detected.